变幻莫测的人脸生成。漫画 / 崔泓

作为一种“泛在”性的存在，数据的安全维护是一个非常复杂的系统，面临着数据确权、数据垄断、数据泄露以及数据作假等主要挑战，由此带来的安全风险包括：数据非法跨境流通可能危害国家主权和国家安全；数字信息的过度采集和非法使用，可能侵犯公民的权利和隐私；算法的偏好可能加剧社会的偏见或歧视，威胁公平正义；机器深度学习难以理解人性的道德，无人驾驶汽车紧急避险等智能决策可能威胁特定的人群生命；人机相互交互式产品广泛应用带来的工作、生活、感情的高度依赖，可能威胁社会伦理。

所以说，数据安全不仅是一个技术问题，也是一个安全问题，同时还涉及伦理、法律和国际规则的相关问题。简而言之，如果数据背后代表了个人，就有个人权益的概念；如果数据背后代表的是组织，就涉及知识产权、商业秘密；如果数据背后代表了行业或者国家，就有数据的主权和国家安全这些概念交织在里面。企业需要盘点自己的数据资产，并考虑在数据使用的过程中可能牵扯到哪些权利。

张照龙指出，数据风险点可能出现在数据的产生、收集、存储与传输的各个环节。近几年工信部处理了一些违规 App，这些违规的 App 多数是采集了个人的一些隐私信息。“大家都有过这样的经历，刚刚说了某样东西，某个购物软件就向你做了推荐；或者某个新闻就向你做了推送。这些互联网企业挖掘海量用户数据资源，用于定向推送，产生商业利益。我们的衣食住行变得越来越方便，我们的隐私也就变得越来越少。如何在隐私保护与开发数据资源之间达成某种平衡，一直是各国立法面临的重要问题。与此同时，海量数据集中在少部分平台和公司之中，无形中也增大了大规模数据泄露的风险。近年来数据泄露的事件屡见不鲜，涉及工业制造、政府数据、医疗信息、个人账号、军工情报等诸多领域。”

另外一个不容忽视的问题是数据造假。数据篡改或作假问题日益引起广泛关注。环境监测、金融数据、电商交易、视频网站以及社交平台上的公开数据不时爆出造假新闻，而这些假数据对于依赖数据真实性的行业发展极为不利，更会影响国家相关领域的宏观判断与政策制定。更严重的后果还在于，人工智能和机器学习的应用中，无论是算法还是机器学习，都基于海量数据，如果基于被篡改的数据与作假的数据，算法的有效性与学习效果可想而知会出现多么大的偏差。一个最现成的案例就是人脸识别技术。早期的人脸识别可能对白种人或者亚洲人的识别效果比较好，但是对于非洲人、黑人的识别效果比较差，这就涉及数据偏差和歧视问题。

目前的人工智能应用场景中，个人生物识别信息以其独特性、唯一性、可数据化和便携性而被广泛应用在生活的方方面面。指纹锁、小区人脸识别门禁、疫苗注射登记乃至于天网系统都与个人生物识别信息密切相关。而在刚刚结束的 2021 世界人工智能大会上，参与人工智能安全高端对话的复旦大学计算机学院副院长杨珉透露，很多国家级政务平台，包括头部 App 厂商的生物特征身份登录，都存在着一定的问题。

此外，利用人工智能的“深度伪造”技术对生物信息进行替换、合成和调整，已经足以实施“换脸术”“变声术”，甚至造出集合上百人特征的“合成脸”，实施各种犯罪行为。这些深度伪造技术足以引发政治风险、社会风险乃至影响国家安全和国际社会安全。

“现在很火的自动驾驶汽车、无人驾驶，如果当它面临投毒攻击或者定向攻击，或者它本身的算法出现问题的时候，很容易导致车祸出现人身伤害，这也是和我们的传统计算机安全不太一样的地方，人工智能的数据安全出现问题的时候，可能会引发社会安全乃至国家安全问题。”张照龙说。

安永网络安全及隐私保护咨询大中华区合伙人高轶峰在 2021 世界人工智能安全高端对话上感慨，过去一周国家一系列监管措施的出台，让很多企业第一次把数据安全真正视为企业生存的一条生命线了。“这对所有做安全的人来说，都是一个好消息，我们不再需要教育市场和教育管理层了。”